

# NAVIGATING THE COMPETITIVE LANDSCAPE

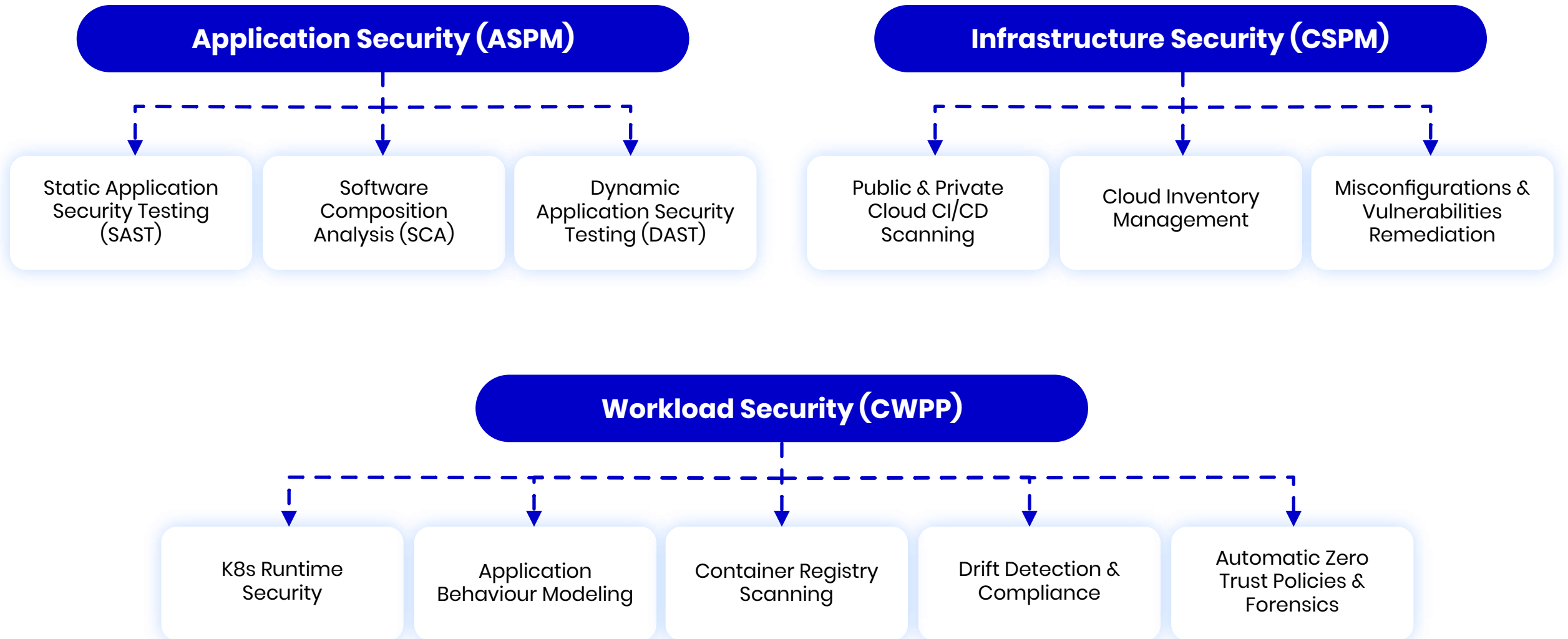


VS

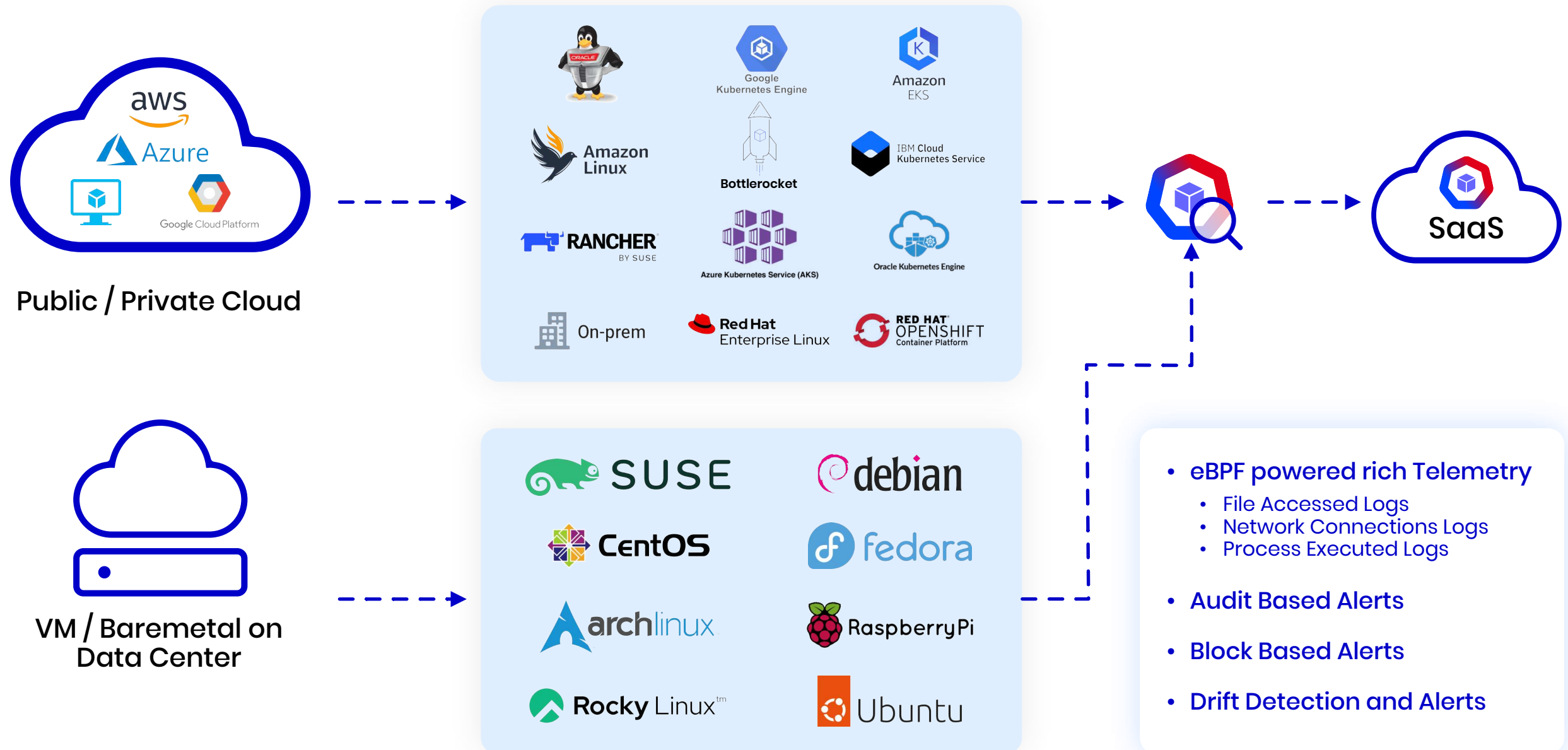


**KEY DIFFERENTIATORS**

# What we offer



# We can secure Multi-Cloud, Air-Gapped & On-Prem



# Capabilities



## CWPP

Industry Standard (eBPF) Based Kernel Telemetry



Inline Security (as opposed to post-attack mitigation)



Provides only detection capabilities

Industry Standard (LSM) Based Security Enforcement



Focused on real-time detection rather than mitigation

Supported Platforms - Linux & k8s



Suse, Debian, Ubuntu, Red Hat, Fedora, Rocky Linux, Amazon Linux, Raspberry Pi, ArchLinux, Alibaba Cloud Linux; K8s - on-prem (k3s, micro k8s, kubeadm), GKE, AKS, OKE, Bottle Rocket, IBM, Graviton, Rancher, Openshift, Oracle Ampere; Microshift, VMWare Tanzu, MKE, DOKS, Vm/Bare Metal



Debian v10 and above, Ubuntu v18 and above, CentOS, RHEL, SUSE, Fedora, Linux Mint, Amazon Linux, Bottlerocket, Google Container optimized OS, Oracle Linux, Amazon EKS, ECS, Azure AKS, Google GKE, OpenShift, IBM Cloud Kubernetes Service(IKS), MKE, VMWare Tanzu.

# Capabilities



## CWPP

Windows Support



Can be provided through Xcitium, Scanning is possible through integrations with tools like Nessus



Observability



Using eBPF



Using eBPF

Application Behavior



Automatic Policies



# Capabilities



## CWPP

Drift Detection



Hardening



Application and Kernel



Policy Lifecycle Management



Network micro-segmentation



Using eBPF



# Capabilities



## CWPP

File Integrity Monitoring



Can also prevent modifications



Only monitoring

Cluster Benchmarking



Deployment



DaemonSet. No changes are required in containers  
Systemd for non-containerized env



DaemonSet. No changes are required in containers  
Standalone binary for non-containerized env

Admission Controller



Support for Serverless, VM, Baremetal, k8s



does not support bare-metal

# Capabilities



## CSPM

Asset Inventory



AWS, Azure, GCP



AWS, Azure, GCP

Cloud misconfigurations



Drift detection



Anomaly detection





## CSPM

Monitoring and alerts



Compliance



Offers 33+ Compliance frameworks including NIST, CIS, MITRE, ISO 27001, PCI, HIPAA, and more



Includes NIST, CIS, PCI, GDPR, and more.

Agentless Scanning



Remediation Suggestions



# Capabilities



## CSPM

Auto Remediation



Can integrate with OPA to automate compliance enforcement

Risk Correlation



## DSPM

Data Security



## ASPM

Registry Scan



ECR, GCR, Nexus, Docker Hub, ACR, Harbor, Quay, jFrog, OpenShift, GAR.



ECR, Jfrog, ACR, ICR, Quay, Harbor, GAR, GCR, Nexus

Malware Scan



Requires Integration



IaC Scanning



Identify 3rd Party dependencies and their vulnerabilities (SCA)



# Capabilities



## ASPM

Generate SBOM



Scan for vulnerability in code as it is built (SAST)



Evaluate applications for vulnerabilities(DAST)



Integrate with CI/CD for shift left automation



Prioritization




# Capabilities



## CIEM

Identify overprivileged IAM roles

  
In Roadmap




## KSPM

Observability of effective privileges



Query identity issues (KIEM)



  
Offer identity-related issues in KSPM

# Capabilities



## KSPM

Detect user activity and authentication errors



Compliance benchmarking



CIS for managed clusters only

## Deployment

On-Prem/Air Gapped



# Capabilities



## Deployment

SaaS



Open Source Community Support



## Integrations

Ticketing/Workflow/Channels



Jira Cloud/Server, FreshService, ConnectWise, Splunk, RSyslog, AWS Cloudwatch, Azure Sentinel, Email, Slack



Jira, ServiceNow, Splunk, Elasticsearch, Syslog, Okta.

## Integrations

Security Findings



**Software:** CLOC, Fortify, Snyk, SonarQube, Sonatype, Trivy, Veracode  
**Container:** Clair/ECR, Snyk, Trivy.  
**Web App:** Burp, Droopescan, Zap



Can integrate with snyk and docker scout

## Gen-AI/LLM-based cloud security assistance

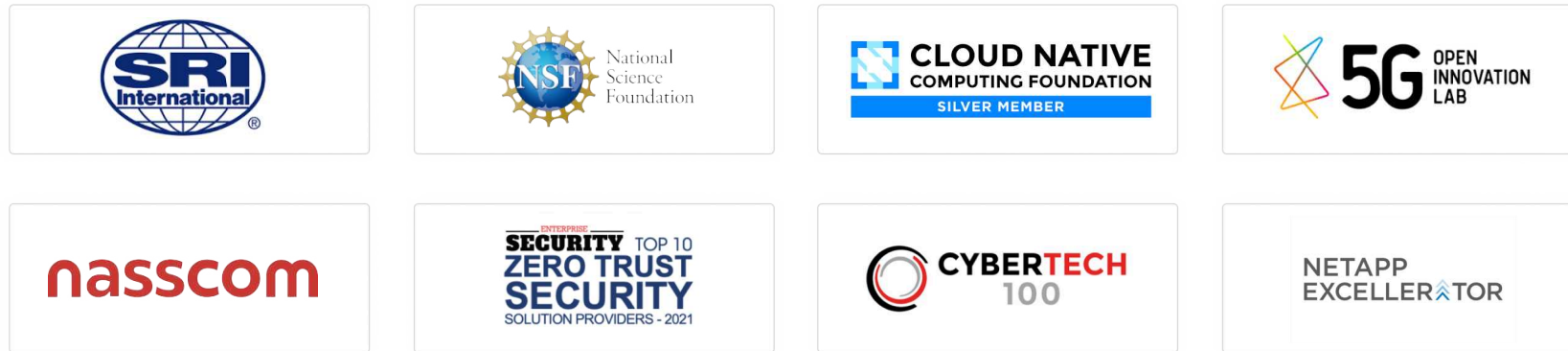
AI/LLM-based chatbot



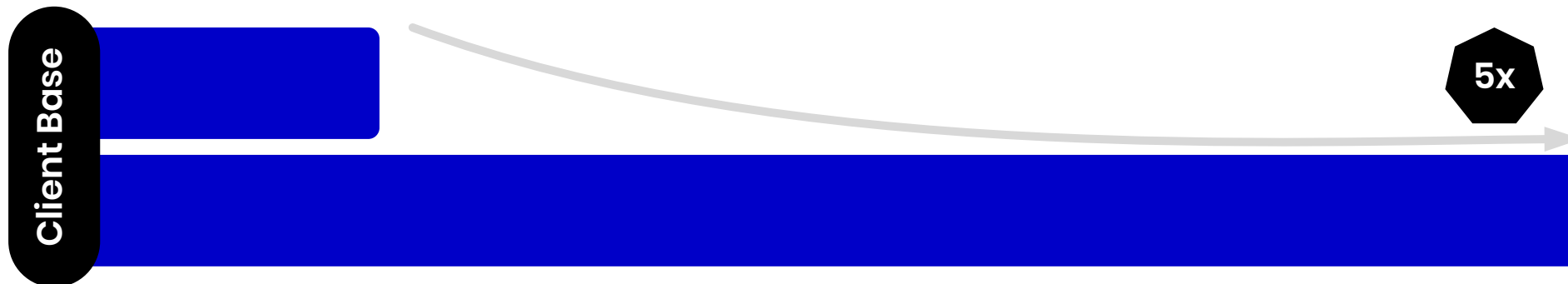


# Our Recognitions 1/3

We feel very privileged to have received numerous awards and recognitions



Our client base has grown 5x this year



# Our Recognitions 2/3



**OLFEDGE** 🔍 ☰

## AccuKnox joins mimik Technologies, IBM as Open Horizon project partner

By Joe Pearson | May 22, 2023 | No Comments

The [Open Horizon](#) project, contributed by IBM to the Linux Foundation, developed a solution to automate complex edge computing workload and analytics placement decisions. Open Horizon also provides end-to-end security for the deployment process using security best practices. As a result of its rigorous adherence to recommended procedures, the Open Horizon project recently earned the OpenSSF Best Practices



August 1, 2022

## AccuKnox Inc. joins the VMWare Technology Alliance Partner Program and announces the availability of AccuKnox Runtime Security on VMWare Marketplace

MENLO PARK, Calif. and CUPERTINO, Calif., Aug. 1, 2022 /PRNewswire/ -- AccuKnox Inc, The Zero Trust runtime security platform for Kubernetes, today announced it has joined



## Secure Bottlerocket deployments on Amazon EKS with KubeArmor

by Raj Seshadri | on 20 OCT 2022 | in [Amazon Elastic Kubernetes Service](#), [Containers](#), [Customer Solutions](#), [Technical How-To](#) | [Permalink](#) | [Share](#)

### Introduction

[Bottlerocket](#) is a security focused operating system (OS) image that provides out-of-the-box security options to protect host or worker nodes. While Bottlerocket is useful, the



September 13, 2022

## AccuKnox Selected to Join 5G Open Innovation Lab Development Program, Bringing Zero Trust Security to the 5G Ecosystem

# Our Recognitions 3/3

## Optimized for Intel® Smart Edge



KubeArmor

## Zero Trust Cloud Native Application Protection

### Overview of KubeArmor

KubeArmor is a cloud-native runtime security enforcement system that restricts the behavior (such as process execution, file access, and networking operations) of containers and nodes (VMs) at the system level. KubeArmor leverages [Linux security modules \(LSMs\)](#) such as [AppArmor](#), [SELinux](#), or [BPF-LSM](#) to enforce the

KubeArmor support for Oracle Container Engine for Kubernetes (OKE)

KubeArmor Support for Oracle Container Engine for Kubernetes (OKE)



- PRODUCT ▾
- SOLUTIONS ▾
- DOCS
- ABOUT ▾
- CONTACT
- BLOG
- GET A DEMO

June 19, 2023

### KubeArmor - an Open Source project by AccuKnox with 500k+ downloads, is now available in AWS Marketplace

**CUPERTINO, Calif., June 22, 2023 /PRNewswire/** — AccuKnox™, a leader in Zero Trust CNAPP (Cloud Native Application Protection Platform), today announced KubeArmor™, an Open Source CNCF Kubernetes run-time security project, is now available in AWS Marketplace -- a digital catalog with thousands of software listings from independent software vendors (ISVs) that make it easy to find, test, buy, and deploy software that runs on Amazon Web Services (AWS).

AccuKnox is now available in AWS Marketplace to provide application teams with greater access and scalability for Open Source CNCF Kubernetes run-time security project, KubeArmor.

"By making KubeArmor available in AWS Marketplace, we are taking steps towards achieving our goal of making Zero Trust Kubernetes Security project KubeArmor more widely available to the AWS community," said Rahul Jadhav, AccuKnox co-founder and chief technology & product officer.

### AccuKnox Forges Partnership with Touchstone Security, Managed Security Services Provider (MSSP) to deliver comprehensive Cloud Security Services

deliver comprehensive Cloud Security Services

**CUPERTINO, CA – July 24, 2023** AccuKnox, Inc announced a partnership with Touchstone Security, a seasoned Managed Security Services Provider (MSSP).

AccuKnox® offers a comprehensive Cloud Native Application Protection Platform (CNAPP) solution. AccuKnox delivers Zero Trust Security for Multi-cloud, Private/Public Cloud environments. In keeping with CI/CD best practices, AccuKnox focuses on finding vulnerabilities earlier in the software development process. AccuKnox is a comprehensive solution that delivers Cloud Security, Code Scanning, Container Security, API security, Host Security, Network Security and Kubernetes orchestration security. AccuKnox is a core contributor to Kubernetes run-time security solution KubeArmor which has been adopted by CNCF and has achieved 500,000+ downloads. AccuKnox, Zero Trust Enterprise CNAPP is anchored on KubeArmor and is an integrated Cloud Native Security platform that includes:

- CSPM/KSPM (Cloud/Kubernetes Security Posture Management)
- CWPP (Cloud Workload Protection Platform)
- CIEM/KIEM (Cloud/Kubernetes Identity and Entitlement Management)

# Trusted by Global Innovators



# World's Leading CISOs can't be wrong..

**70%** INCREASE IN CRITICAL  
ISSUES RESOLUTION

**5** SIEM TOOLS  
INTEGRATED

“ We are very pleased to partner with a Modern, Cloud Native, Zero Trust CNAPP innovator like AccuKnox. Zero Trust security is a commitment we have to our customers. Their work with AWS furthers the value that AccuKnox can deliver to us.”



**80%** EFFICIENCY IN  
HANDLING FALSE  
POSITIVE ALERTS

**5** MINUTES TO SOLVE  
KNOWN  
VULNERABILITIES

“ Zero Trust security is Clint Health's imperative and commitment we have to our customers. AccuKnox's leading product combined with their successful track record of partnering with their customers forms the foundation for this objective.”



**50%** TIME REDUCED IN  
HANDLING CI/CD  
PIPELINE ISSUES

**1** MINUTE TO OBTAIN  
INSTANT REPORTS

“ Our client, a Large European CyberSecurity agency, was looking for a Zero Trust Security Solution that supports Private Cloud platforms. Our win is a clear testament to the value our clients see in this partnership.”



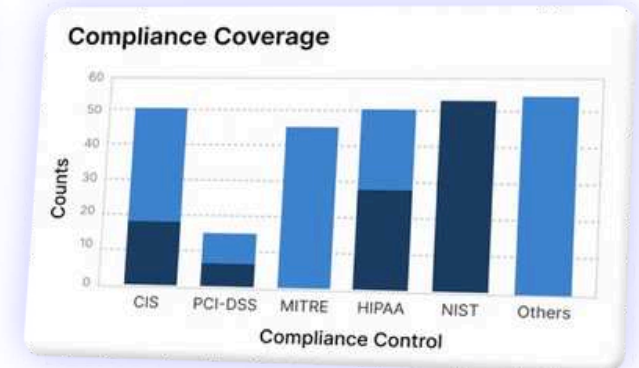
# Reasons to choose us

## Single Platform

- ✓ Code to cloud - "Shift Left" Security
- ✓ GRC Conformance Tool
- ✓ Zero Day attack defence
- ✓ Operator Error Protection
- ✓ Easy to integrate with SIEM/SOC and DevOPs
- ✓ Easy to integrate third-party scanning tools

## Multiplatform

- ✓ AWS, Azure, Google, IBM, Oracle
  - Available on AWS Marketplace
- ✓ Private Cloud
- ✓ Air-Gapped & On-premise
- ✓ Edge Computing
  - Chosen by Google & US military to secure 5G private networks
- ✓ Supports Hybrid Deployments



**Policies**

Policy Name	Category	Status	Cluster	Namespace	Selector Labels
autopol-system-414 (v.1) Kubernetes Network	Discovered	Inactive	azure-aks-cluster	wordpress	app=frontend +4
autopol-system-414 (v.1) Cilium Network	Discovered Applied 4hrs ago	Active	test-cluster	kube-system	app=java-ms-cron +4
mysqldump-bin-exec (v.1) KubeArmor	Hardening Applied 5hrs ago	Active	amazon-eks-cluster	wordpress	app=mysql +4
elasticsearch-log-files (v.1) KubeArmor	Hardening	Inactive	test-cluster	default	app=wordpress-poc +4

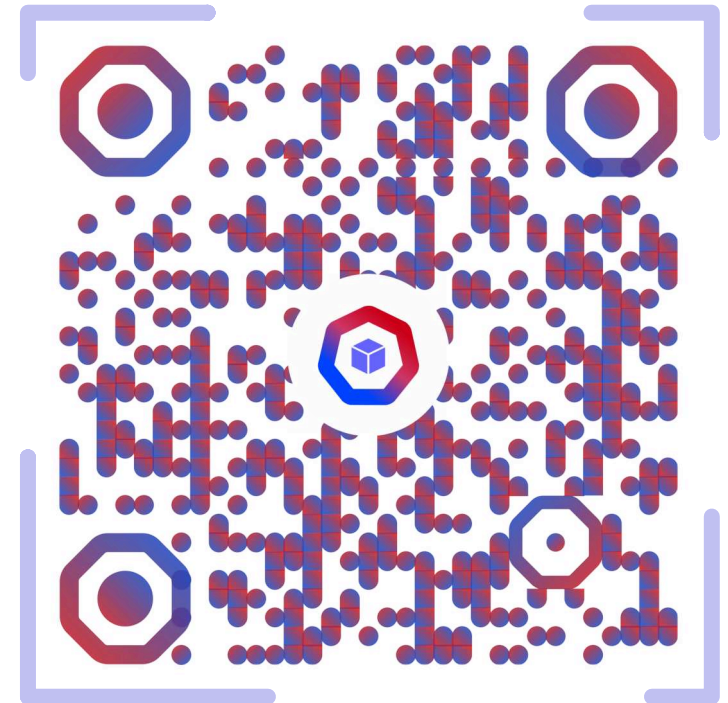
## Competitive Edge

- ✓ No modifications require to the runtime environment
- ✓ Open source agents
- ✓ In Line Prevention instead of traditional Post Attack Mitigation

# Subscribe to AccuKnox CNAPP Free Forever Plan



Available in AWS  
Marketplace



For more: [www.accuknox.com](http://www.accuknox.com)

Email us: [support@accuknox.com](mailto:support@accuknox.com)

[Book a Demo](#)

# THANK YOU!

Follow us on



in

